AP

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/904,010	07/11/2001	Bruce K. Martin JR.	3399P042	1786

26529 7590 04/03/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN/PDC
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 04/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/904,010	**Applicant(s)** MARTIN ET AL.	
	Examiner Kaveh Abrishamkar	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *1/10/2006*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on January 10, 2006. Claims 1, 15, 27, and 40 are currently amended. Claims 1-55 are currently being considered.

Response to Arguments

Applicant's arguments filed January 10, 2006 have been fully considered but they are not persuasive for the following reasons;

Regarding amended independent claim 1, the Applicant argues that the Cited Prior Art (CPA, Soursa et al. (U.S. Patent Publication US 2002/0194584 A1), does not teach a "second provisioning system, which comprises a provisioning server." This argument is not found persuasive. The CPA discloses "a provisioning network" (first provisioning server) which communicates with an agent (second provisioning server) regarding tasks (provisioning) that need to be performed on its device (paragraphs 45-47). The act of provisioning is performed first by the "provisioning network" by instructing the agent of commands that the agent will perform on a device (second act of provisioning). The applicant argues that this agent cannot be a server is within the same device that is being provisioned. However, using www.whatis.com, the definition of a server is "a computer program that provides services to other computer programs (and their users) ***in the same*** or other computers." Based on the definition of a server, it is asserted that the agent on the device can be interpreted as a "second provisioning server" as it does provision the device that is it resident on.

Furthermore, the Applicant argues that the CPA does not teach "a provisioning message that specifies a secondary TPD or provisioning system authorized to provision the mobile device and an identifier of one or more parameters which the secondary TPD is authorized to provision." This argument is not found persuasive. The CPA discloses "the agent communicates with the provisioning network 31 to obtain commands regarding tasks that need to be performed on its device" (paragraph 47). The commands can be viewed as the provisioning message as they contain instructions on how to provision the device. Therefore, it is asserted that the CPA does teach the above limitation.

Furthermore, the Applicant argues that the CPA, Soursa et al. (U.S. Patent Publication US 2002/0194584 A1) in view Ramasubramani et al. (U.S. Patent No. 6,233,577), does not teach using the primary provisioning server to provision a digital certificate of the first and second provisioning servers onto the device. This argument is not found persuasive. As disclosed in the previous Office Action, Soursa does not teach "provisioning digital certificates." Ramasubramani teaches using "digital certificates" (column 4 lines 29-30) in devices. Ramasubramani was used to teach the use of digital certificates and not the provisioning of devices. Soursa teaches that "information stored in this database comprises all data that is necessary to provision a device" (paragraph 47) and that this information can include software components that are installed on each device, and logical information about the device (paragraph 47).

This information can include any type of logical information including a digital certificate, which would be used to provide "the most secure use of authentication" (Ramasubramani: column 4 lines 29-31). Therefore, it is asserted that the CPA does teach the above limitation.

Therefore, it is respectfully asserted that the CPA does teach the above limitations, and the rejection is respectfully maintained for the pending claims as given below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-6 and 39 are rejected under 35 U.S.C. 102(e) as being anticipated by Suorsa et al. (U.S. Patent Publication No. US 2002/0194584 A1).

Regarding claim 1, Suorsa discloses:

A method comprising:

operating a first provisioning system authorized to provision a processing device on a network, wherein the first provisioning system is within a trusted environment (paragraphs 13-14, 47-48), wherein a provisioning system includes a central database with all information relevant to the provisioning of devices; and

using the first provisioning system to authorize a second provisioning system which comprises a provisioning server and is outside the trusted environment to provision the processing device (Figure 7, paragraphs 46-48), wherein agents (second provisioning systems) are instructed by a gateway what commands and parameters to place on the device being provisioned.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Suorsa discloses:

A method as recited in claim 1, wherein said using the first provisioning system to authorize a second provisioning system comprises using the first provisioning system to provision authorization of the second provisioning system in the processing device (Figure 7, paragraphs 46-48), wherein agents (second provisioning systems) are instructed by a gateway what commands and parameters to place on the device being provisioned.

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Suorsa discloses:

A method as recited in claim 2, wherein said using the first provisioning system to authorize a second provisioning system comprises using the first provisioning system to send a provisioning message to the processing device, the provisioning message indicating authorization of the second provisioning system to provision the processing device (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Suorsa discloses:

A method as recited in claim 3, wherein the provisioning message further specifies one or more parameters which the second provisioning system is authorized to provision (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Suorsa discloses:

A method as recited in claim 1, wherein said using the first provisioning system to authorize a second provisioning system comprises using the first provisioning system to send a provisioning message to the processing device, the provisioning message indicating authorization of a plurality of other provisioning systems, including the second provisioning system, to provision the processing device (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Suorsa discloses:

A method as recited in claim 5, wherein the provisioning message further specifies one or more parameters which each of the other provisioning systems is authorized to provision (paragraph 47).

Regarding claim 39, Suorsa discloses:

An apparatus comprising:

means for operating a first provisioning system authorized to provision a processing device on a network, wherein the provisioning system is within a trusted environment (paragraphs 13-14, 47-48), wherein a provisioning system includes a central database with all information relevant to the provisioning of devices; and means for using the first provisioning system to authorize a second provisioning system outside the trusted environment to provision the processing device (Figure 7, paragraphs 46-48), wherein agents (second provisioning systems) are instructed by a gateway what commands and parameters to place on the device being provisioned.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7, 17, 19, 27-29, 31, 40-41, 43-45, 47-49, and 51-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Suorsa et al. (U.S. Patent Publication No. US 2002/0194584 A1).

Claim 7 is rejected as applied above in rejecting claim 1. Suorsa does not explicitly state that the processing device is a mobile device on a wireless network. However, Suorsa states that "the invention can find practical application in any environment where the automated provisioning of computer resources is desirable" (paragraph 29). Particularly, the number of devices is a reason for implementing the provisioning method of Suorsa, and it is well-known that the mobile environment possesses many clients, and in a mobile environment, the automated provisioning would be beneficial due to the large number of devices, that are sparsely located. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to adapt the invention of Suorsa to the mobile wireless environment to simplify and expedite the provisioning of the mobile devices.

Regarding claim 15, Suorsa discloses:

operating a primary trusted provisioning domain (TPD) (paragraphs 13-14, 47-48), wherein a provisioning system includes a central database with all information relevant to the provisioning of devices; and using the primary TPD to provision a device on a network by sending a provisioning message to the device, the provisioning message specifying a secondary TPD authorized to provision the device and an identifier of one or more parameters which the secondary TPD is authorized to provision (Figure 7, paragraphs 46-48), wherein agents (second provisioning systems) are instructed by a gateway what commands and parameters to place on the device being provisioned.

Suorsa does not explicitly state that the processing device is a mobile device on a wireless network. However, Suorsa states that "the invention can find practical application in any environment where the automated provisioning of computer resources is desirable" (paragraph 29). Particularly, the number of devices is a reason for implementing the provisioning method of Suorsa, and it is well-known that the mobile environment possesses many clients, and in a mobile environment, the automated provisioning would be beneficial due to the large number of devices, that are sparsely located. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to adapt the invention of Suorsa to the mobile wireless environment to simplify and expedite the provisioning of the mobile devices.

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Suorsa discloses:

A method as recited in claim 15, wherein the primary TPD is within a trusted environment, and wherein the secondary TPD is outside the trusted environment (paragraph 50).

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Suorsa discloses:

A method as recited in claim 16, wherein the secondary TPD communicates with the mobile device via a second network that is outside the trusted environment (paragraph 50).

Claim 19 is rejected as applied above in rejecting claim 15. Furthermore, Suorsa discloses:

A method as recited in claim 15, wherein the provisioning message specifies a plurality of secondary TPDs authorized to provision the mobile device and one or more parameters which each of the secondary TPDs is authorized to provision (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Regarding claim 27, Suorsa discloses:

A provisioning system comprising:

a processor (paragraph 31);

a data communication device coupled to the processor to communicate data with one or more remote systems (Figure 7, item 38); and a memory coupled to the processor and storing instructions for execution by the processor to cause the provisioning system to provision a device on a network by sending a provisioning message to the device, the provisioning message specifying a second provisioning system authorized to provision the device and an identifier of one or more parameters which the second provisioning system is authorized to provision (Figure 7, paragraphs 46-48), wherein agents (second provisioning systems) are instructed by a gateway what commands and parameters to place on the device being provisioned.

Suorsa does not explicitly state that the processing device is a mobile device on a wireless network. However, Suorsa states that "the invention can find practical application in any environment where the automated provisioning of computer resources is desirable" (paragraph 29). Particularly, the number of devices is a reason for implementing the provisioning method of Suorsa, and it is well-known that the mobile environment possesses many clients, and in a mobile environment, the automated provisioning would be beneficial due to the large number of devices, that are sparsely located. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to adapt the invention of Suorsa to the mobile wireless environment to simplify and expedite the provisioning of the mobile devices.

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Suorsa discloses:

A provisioning system as recited in claim 27, wherein said provisioning system is within a trusted environment, and wherein the second provisioning system is outside the trusted environment (paragraph 50).

Claim 29 is rejected as applied above in rejecting claim 28. Furthermore, Suorsa discloses:

A provisioning system as recited in claim 28, wherein the second provisioning system communicates with the mobile device via a second network that is outside the trusted environment (paragraph 50).

Claim 31 is rejected as applied above in rejecting claim 28. Furthermore, Suorsa discloses:

A provisioning system as recited in claim 27, wherein the provisioning message specifies a plurality of secondary provisioning system authorized to provision the mobile device and one or more parameters which each of the secondary provisioning system is authorized to provision (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Regarding claim 40, Suorsa discloses:

A method of operating a device on a network, the method comprising:

receiving a provisioning message from a first trusted provisioning domain (TPD), the provisioning message specifying a second TPD and indicating a parameter which the second TPD is authorized to provision in the device, the secondary TPD comprising a provisioning server (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device";

storing information identifying the second TPD and the parameter in response to the provisioning message (paragraph 47); and

provisioning the parameter in the device in response to a provisioning message received over a network from the second TPD (paragraph 64).

Suorsa does not explicitly state that the processing device is a mobile device on a wireless network. However, Suorsa states that "the invention can find practical application in any environment where the automated provisioning of computer resources is desirable" (paragraph 29). Particularly, the number of devices is a reason for implementing the provisioning method of Suorsa, and it is well-known that the mobile environment possesses many clients, and in a mobile environment, the automated provisioning would be beneficial due to the large number of devices, that are sparsely located. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to adapt the invention of Suorsa to the mobile wireless environment to simplify and expedite the provisioning of the mobile devices.

Claim 41 is rejected as applied above in rejecting claim 40. Furthermore, Suorsa discloses:

A method as recited in claim 40, wherein the first TPD is within a trusted environment, and the second TPD is outside the trusted environment (paragraph 50).

Claim 43 is rejected as applied above in rejecting claim 40. Furthermore, Suorsa discloses:

A method as recited in claim 40, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, the method further comprising storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Regarding claim 44, Suorsa discloses:

A method of operating a device on a network, the method comprising:

receiving a provisioning message from a remote source, the provisioning message specifying a parameter (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device";

determining whether the remote source is a primary trusted provisioning domain (TPD) (paragraph 50), wherein a digital certificate can be used to attest to the validity of the remote agent;

if the remote source is the primary TPD, provisioning the parameter in the device in response to the provisioning message (paragraph 64).;

if the remote source is not the primary TPD, determining whether the remote source is a secondary TPD authorized to provision the parameter, based on a provisioning authorization previously received by the device from the primary TPD (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device"; and

if the remote source is a secondary TPD authorized to provision the parameter, provisioning the parameter in the device in response to the provisioning message (paragraph 64).

Suorsa does not explicitly state that the processing device is a mobile device on a wireless network. However, Suorsa states that "the invention can find practical application in any environment where the automated provisioning of computer resources is desirable" (paragraph 29). Particularly, the number of devices is a reason for implementing the provisioning method of Suorsa, and it is well-known that the mobile environment possesses many clients, and in a mobile environment, the automated provisioning would be beneficial due to the large number of devices, that are sparsely located. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to adapt the invention of Suorsa to the mobile wireless environment to simplify and expedite the provisioning of the mobile devices.

Claim 45 is rejected as applied above in rejecting claim 44. Furthermore, Suorsa discloses:

A method as recited in claim 44, wherein the primary TPD operates within a trusted environment, and the secondary TPD operates outside the trusted environment (paragraph 50).

Claim 47 is rejected as applied above in rejecting claim 44. Furthermore, Suorsa discloses:

A method as recited in claim 44, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device", the method further comprising storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message (paragraph 47).

Regarding claim 48, Suorsa discloses:

A device configured to operate on a network, the device comprising:

a processor (paragraph 31);

a data communication device coupled to the processor to communicate data with one or more remote systems via the network (Figure 7, item 38); and

a memory coupled to the processor and storing instructions for execution by the processor to configure the device to execute a process comprising receiving a provisioning message from a first trusted provisioning domain (TPD) via the network, the provisioning message specifying a second TPD and indicating a parameter which the second TPD is authorized to provision in the device (Figure 7, paragraphs 46-48), wherein agents (second provisioning systems) are instructed by a gateway what commands and parameters to place on the device being provisioned;

storing information identifying the second TPD and the parameter in response to the provisioning message (paragraph 47); and

provisioning the parameter in the mobile device in response to a provisioning message from the second TPD (paragraph 64).

Suorsa does not explicitly state that the processing device is a mobile device on a wireless network. However, Suorsa states that "the invention can find practical application in any environment where the automated provisioning of computer resources is desirable" (paragraph 29). Particularly, the number of devices is a reason for implementing the provisioning method of Suorsa, and it is well-known that the mobile environment possesses many clients, and in a mobile environment, the automated provisioning would be beneficial due to the large number of devices, that are sparsely located. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to adapt the invention of Suorsa to the mobile wireless environment to simplify and expedite the provisioning of the mobile devices.

Claim 49 is rejected as applied above in rejecting claim 48. Furthermore, Suorsa discloses:

A mobile device as recited in claim 48, wherein the first TPD is within a trusted environment, and the second TPD is outside the trusted environment (paragraph 50).

Claim 51 is rejected as applied above in rejecting claim 48. Furthermore, Suorsa discloses:

A mobile device as recited in claim 48, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, and wherein the process further comprises storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.

Regarding claim 52, Suorsa discloses:

A device configured to operate on a network, the device comprising:

a processor (paragraph 31);

a data communication device coupled to the processor to communicate data with one or more remote systems via the wireless network (Figure 7, item 38); and a memory coupled to the processor and storing instructions for execution by the processor to configure the mobile device to execute a process comprising receiving a provisioning message from a remote source, the provisioning message specifying a parameter (Figure 7, paragraphs 46-48), wherein agents (second provisioning systems) are instructed by a gateway what commands and parameters to place on the device being provisioned;

determining whether the remote source is a primary trusted provisioning domain (TPD) (paragraph 50), wherein a digital certificate can be used to attest to the validity of the remote agent;

if the remote source is the primary TPD, provisioning the parameter in the mobile device in response to the provisioning message (paragraph 64);

if the remote source is not the primary TPD, determining whether the remote source is a secondary TPD authorized to provision the parameter, based on a provisioning authorization previously received by the mobile device from the primary TPD (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device"; and

if the remote source is a secondary TPD authorized to provision the parameter, provisioning the parameter in the mobile device in response to the provisioning message (paragraph 64).

Claim 53 is rejected as applied above in rejecting claim 52. Furthermore, Suorsa discloses:

A mobile device as recited in claim 52, wherein the primary TPD operates within a trusted environment, and the secondary TPD operates outside the trusted environment (paragraph 50).

Claim 55 is rejected as applied above in rejecting claim 52. Furthermore, Suorsa discloses:

A mobile device as recited in claim 52, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, and wherein the process further comprises storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message (paragraph 47).

4. Claims 8-14, 18, 20-26, 30,32-38,42,46,50, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Suorsa et al. (U.S. Patent Publication No. US 2002/0194584 A1) in view of Ramasubramani et al. (U.S. Patent 6,233,577).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Suorsa discloses:

A method as recited in claim 7. Suorsa does not explicitly disclose using a digital signature to provision the mobile device. Ramasubramani discloses using a digital signature to provision the mobile device (column 4 lines 29-30). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 9 is rejected as applied above in rejecting claim 8. Suorsa does not disclose using the digital signature to authentication the source of the provisioning message. Ramasubramani discloses using the digital signature to authenticate the source of the provisioning message (column 4 lines 29-30). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 10 is rejected as applied above in rejecting claim 8. Suorsa does not explicitly disclose using the first provisioning system to provision the mobile device with a digital certificate identifying the first provisioning system. Ramasubramani discloses using the first provisioning system to provision the mobile device with a digital certificate identifying the first provisioning system (column 7 lines 10-14). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 11 is rejected as applied above in rejecting claim 8. Suorsa does not explicitly disclose using the first provisioning system to provision the mobile devices with a digital certificate identifying the second provisioning system. Ramasubramani discloses using the first provisioning system to provision the mobile device with a digital certificate identifying the second provisioning system (column 7 lines 10-14). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Suorsa discloses:

A method as recited in claim 11, wherein the second provisioning system is on a second network that is outside the trusted environment and separate from, but coupled to, the wireless network (paragraph 50).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Suorsa discloses:

A method as recited in claim 12, wherein the first provisioning system has unrestricted authorization to provision the mobile device, and the authorization of the second provisioning system to provision the mobile device is regulated from the first provisioning system (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device", the method further comprising storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message (paragraph 47).

Claim 14 is rejected as applied above in rejecting claim 8. Suorsa does not explicitly disclose a using the first provisioning system to provision the mobile device with digital certificates identifying a plurality of other provisioning systems. Ramasubramani discloses using the first provisioning system to provision the mobile device with digital certificates identifying a plurality of other provisioning systems (column 7 lines 10-14). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 18 is rejected as applied above in rejecting claim 16. Suorsa does not explicitly disclose using the primary TPD system to provision the mobile device with a digital certificate identifying the secondary TPD to enable the secondary TPD to provision the mobile device using a digital signature. Ramasubramani discloses using the primary TPD system to provision the mobile device with a digital certificate identifying the secondary TPD to enable the secondary TPD to provision the mobile device using a digital signature (column 7 lines 10-14; column 8 lines 1-5). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Regarding claim 20, Suorsa discloses:

A method comprising:

operating a primary provisioning server within a predefined trusted environment, the primary provisioning server having authorization to provision a plurality of devices on a network (paragraphs 13-14, 47-48), wherein a provisioning system includes a central database with all information relevant to the provisioning of devices;

using the primary provisioning server to provision the devices with information indicating to the mobile devices authorization of the secondary provisioning server to provision the devices (Figure 7, paragraphs 46-48), wherein agents (second provisioning systems) are instructed by a gateway what commands and parameters to place on the device being provisioned.

Suorsa does not explicitly state that the processing device is a mobile device on a wireless network. However, Suorsa states that "the invention can find practical application in any environment where the automated provisioning of computer resources is desirable" (paragraph 29). Particularly, the number of devices is a reason for implementing the provisioning method of Suorsa, and it is well-known that the mobile environment possesses many clients, and in a mobile environment, the automated provisioning would be beneficial due to the large number of devices, that are sparsely located. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to adapt the invention of Suorsa to the mobile wireless environment to simplify and expedite the provisioning of the mobile devices.

Furthermore, Suorsa does not explicitly disclose using the primary provisioning server to provision a digital certificate of the primary provisioning server in each of the mobile devices, and using the primary provisioning server to provision a digital certificate of a secondary provisioning server in the mobile devices. Ramasubramani discloses using the primary provisioning server to provision a digital certificate of the primary provisioning server in each of the mobile devices (column 7 lines 10-14), and using the primary provisioning server to provision a digital certificate of a secondary provisioning server in the mobile devices (column 7 lines 10-14). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 21 is rejected as applied above in rejecting claim 20. Suorsa does not explicitly disclose a method wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers. Ramasubramani discloses a method wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers (column 4 lines 29-30). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 22 is rejected as applied above in rejecting claim 20. Furthermore, Suorsa discloses:

A method as recited in claim 20, further comprising using the primary provisioning server to specify one or more parameters which the secondary provisioning server is authorized to provision in the mobile device (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Claim 23 is rejected as applied above in rejecting claim 20. Furthermore, Suorsa discloses:

A method as recited in claim 20, further comprising using the primary provisioning server to provision the mobile devices with information indicating authorization of a plurality of secondary provisioning servers to provision the mobile devices (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Suorsa discloses:

A method as recited in claim 23, further comprising using the primary provisioning server to specify one or more parameters which each of the secondary provisioning servers is authorized to provision in the mobile devices (paragraph 47), wherein the agents (second provisioning system) receives instructions from the first provisioning system including "commands regarding tasks that need to be performed on its device."

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Suorsa discloses:

A method as recited in claim 24, wherein said using the primary provisioning server to specify one or more parameters comprises assigning each of the secondary provisioning servers provisioning authorization of a different scope (paragraph 47).

Claim 26 is rejected as applied above in rejecting claim 20. Furthermore, Suorsa discloses:

A method as recited in claim 20, wherein the primary provisioning server has unrestricted authorization to provision the mobile devices, and authorization of the secondary provisioning server to provision the mobile devices is regulated by the primary provisioning server (paragraph 47).

Claim 30 is rejected as applied above in rejecting claim 28. Suorsa does not explicitly disclose using the primary TPD system to provision the mobile device with a digital certificate identifying the secondary TPD to enable the secondary TPD to provision the mobile device using a digital signature. Ramasubramani discloses using the primary TPD system to provision the mobile device with a digital certificate identifying the secondary TPD to enable the secondary TPD to provision the mobile device using a digital signature (column 7 lines 10-14, column 8 lines 1-5). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Regarding claim 32, Suorsa discloses:

A machine-readable program storage medium storing instructions which, when executed in a processing system, configure the processing system to operate as a primary provisioning server within a predefined trusted environment, the primary provisioning server having authorization to provision a plurality of devices on a network, such that the instructions configure the processing system to execute a process comprising:

provisioning the mobile devices with information indicating to the mobile devices authorization of the secondary provisioning server to provision the mobile devices (paragraph 47).

Suorsa does not explicitly state that the processing device is a mobile device on a wireless network. However, Suorsa states that "the invention can find practical application in any environment where the automated provisioning of computer resources is desirable" (paragraph 29). Particularly, the number of devices is a reason for implementing the provisioning method of Suorsa, and it is well-known that the mobile environment possesses many clients, and in a mobile environment, the automated provisioning would be beneficial due to the large number of devices, that are sparsely located. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to adapt the invention of Suorsa to the mobile wireless environment to simplify and expedite the provisioning of the mobile devices.

Furthermore, Suorsa does not explicitly disclose using the primary provisioning server to provision a digital certificate of the primary provisioning server in each of the mobile devices, and using the primary provisioning server to provision a digital certificate of a secondary provisioning server in the mobile devices. Ramasubramani discloses using the primary provisioning server to provision a digital certificate of the primary provisioning server in each of the mobile devices (column 7 lines 10-14), and using the primary provisioning server to provision a digital certificate of a secondary provisioning server in the mobile devices (column 7 lines 10-14). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 33 is rejected as applied above in rejecting claim 32. Suorsa does not explicitly disclose a method wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers. Ramasubramani discloses a method wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers (column 4 lines 29-30). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 34 is rejected as applied above in rejecting claim 32. Furthermore, Suorsa discloses:

A machine-readable program storage medium as recited in claim 32, wherein the process further comprises specifying one or more parameters which the secondary provisioning server is authorized to provision in the mobile devices (paragraph 47).

Claim 35 is rejected as applied above in rejecting claim 32. Furthermore, Suorsa discloses:

A machine-readable program storage medium as recited in claim 32, wherein the process further comprises provisioning the mobile devices with information indicating authorization of a plurality of secondary provisioning servers to provision the mobile devices (paragraph 47).

Claim 36 is rejected as applied above in rejecting claim 35. Furthermore, Suorsa discloses:

A machine-readable program storage medium as recited in claim 35, wherein the process further comprises specifying one or more parameters which each of the secondary provisioning servers is authorized to provision in the mobile devices (paragraph 47).

Claim 37 is rejected as applied above in rejecting claim 36. Furthermore, Suorsa discloses:

A machine-readable program storage medium as recited in claim 36, wherein said specifying one or more parameters comprises assigning each of the secondary provisioning servers provisioning authorization of a different scope (paragraph 47).

Claim 38 is rejected as applied above in rejecting claim 32. Furthermore, Suorsa discloses:

A machine-readable program storage medium as recited in claim 32, wherein the primary provisioning server has unrestricted authorization to provision the mobile devices, and authorization of the secondary provisioning server to provision the mobile devices is regulated by the primary provisioning server (paragraph 47).

Claim 42 is rejected as applied above in rejecting claim 41. Suorsa does not explicitly disclose receiving a digital certificate of the second TPD from the first TPD and using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD. Ramasubramani discloses a method of receiving a digital certificate of the second TPD from the first TPD (column 4 lines 29-30) and using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD (column 4 lines 29-30). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 46 is rejected as applied above in rejecting claim 44. Suorsa does not explicitly disclose receiving a digital certificate of the second TPD from the first TPD and using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD. Ramasubramani discloses a method of receiving a digital certificate of the second TPD from the first TPD (column 4 lines 29-30) and using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD (column 4 lines 29-30). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 50 is rejected as applied above in rejecting claim 49. Suorsa does not explicitly disclose receiving a digital certificate of the second TPD from the first TPD and using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD. Ramasubramani discloses a method of receiving a digital certificate of the second TPD from the first TPD (column 4 lines 29-30) and using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD (column 4 lines 29-30). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Claim 54 is rejected as applied above in rejecting claim 52. Suorsa does not explicitly disclose receiving a digital certificate of the second TPD from the first TPD and using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD. Ramasubramani discloses a method of receiving a digital certificate of the second TPD from the first TPD (column 4 lines 29-30) and using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD (column 4 lines 29-30). It would have been obvious to combine the teachings of Ramasubramani with the method of Suorsa in order to utilize the most secure use of authentication (column 4 lines 29-30).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
03/22/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER
3/26/06